Remittance Strategy for Paper Check Conversion (RS-PCC) –
Privacy Impact Assessment (PIA), Milestone 4B

PIA Approval Date: December 6, 2007

System Overview

Remittance Strategy for Paper Check Conversion (RS-PCC) enables the Consolidated Campuses, Taxpayer Assistance Centers (TACs) and Revenue Officers (ROs) to electronically process paper remittances at the point of receipt. Using equipment at these locations, the employee can scan the check and the payment voucher. The equipment captures the image and necessary data on each document. The data is forwarded to the Federal Reserve payment system for immediate deposit. Confirmations are returned, enabling the subsequent accounting actions to occur, including the withdrawal of the check amount and crediting payments to the taxpayer's account.

Data in the System

1. Generally describe the information to be used in the system in each of the following categories: Taxpayer, Employee, and Other.

Taxpayer – The following remittance data is collected on the Taxpayer:

- Check Data
  - Check Number
  - Account Number
  - Routing Number
  - Dollar Amount
- Name
- Taxpayer Identification Number (TIN)
- Transaction Date
- Document Locator Number (DLN)

Additional information may be included on the check by the taxpayer, but is not specifically requested or required by the system. Typical data elements that may be added to the check are:

- Social Security Number (SSN)
- Address

Employee – Data which will be collected on the employee during authentication includes:

- Standard Employee ID (SEID)
- Password

Data which will be collected on employees in audit trails:

- SEID
- Date and time of the event
- Type of event
- Outcome status

Other – Checks are occasionally submitted by State attorneys or trustees on behalf of the taxpayer.

2. What are the sources of the information in the system?
Data elements in RS-PCC are provided by other IRS systems, taxpayers, employees, and by the Federal Reserve Bank (FRB) via Financial Management Service Electronic Verification and Imaging System (FMS ELVIS). No information is gathered from state and local agencies.

Data elements provided by IRS systems include:

- **Data Element:** Master File Tax Code (MFT)
- **Potential IRS Source:** The data elements are anticipated to come from either Automated Insolvency System (AIS) or IDRS.
- **Type of Interface:** Manual (no interconnection)

- **Data Element:** Document Locator Number (DLN)
- **Potential IRS Source:** EFTPS
- **Type of Interface:** Electronic

- **Data Element:** Trace ID
- **Potential IRS Source:** EFTPS
- **Type of Interface:** Electronic

- **Data Element:** Tax Period
- **Potential IRS Source:** Not currently determined. The data elements are anticipated to come from either Automated Insolvency System (AIS) or IDRS. Depending on the type of activity they may go to either system.
- **Type of Interface:** Manual (no interconnection)

- **Data Element:** Taxpayer Identification Number (TIN)
- **Potential IRS Source:** Not currently determined. The data elements are anticipated to come from either Automated Insolvency System (AIS) or IDRS
- **Type of Interface:** Manual (no interconnection)

- **Data Element:** Name Control
- **Potential IRS Source:** Not currently determined. The data elements are anticipated to come from either Automated Insolvency System (AIS) or IDRS
- **Type of Interface:** Manual (no interconnection)

Taxpayer data elements are gathered from the image of the check which is scanned in. Data elements provided directly from the taxpayer include:

- Check Data
    - Check Number
    - Account Number
    - Routing Number
    - Dollar Amount
- Name
- Taxpayer Identification Number (TIN)
- Received Date

Additional information may be included on the check by the taxpayer, but is not specifically requested or required by the system. Typical data elements that may be added to the check are:

- TIN
- Address

Data elements provided by the employee include:
- RS-PCC user ID and/or
- SEID

Data elements provided by the Federal Reserve Bank via ELVIS include:
- Deposit ticket number
- Deposit amount

Data elements provided by the paper check conversion (PCC) over-the-counter (OTC) client assigns an Item Reference Number (IRN) to a deposit ticket which is sent to RS-PCC and is used to confirm which tickets have been deposited.

2.a. What IRS files and databases are used?
RS-PCC is interconnected to the following IRS systems:
- Remittance Transaction Research (RTR)
- Electronic Federal Tax Payment System (EFTPS)

Data elements provided by the IRS include:
- MFT
- DLN
- Tax Period
- TIN
- Trace ID
- Name

2.b. What Federal Agencies are providing data for use in the system?
RS-PCC receives data from Financial Management Service Electronic Verification and Imaging System (ELVIS). ELVIS interfaces with the Federal Reserve Bank. The FRB uses the information to electronically debit the check-writer's account via the Automated Clearing House (ACH), credits the IRS account in CA$H-LINK, and returns a confirmed deposit ticket (SF 215) and Item Reference Number (IRN) for each transaction to the RS-PCC system via ELVIS.
Data elements provided by the ELVIS include:
- Deposit ticket number
- Deposit amount
- Item Reference Number

2.c. What State and Local Agencies are providing data for use in the system?
No State or Local Agencies will be providing data for use in the system.

2.d. From what other third party sources will data be collected?
Checks are occasionally submitted by State attorneys or trustees on behalf of the taxpayer

2.e. What information will be collected from the taxpayer/employee?

Taxpayer – Taxpayer data elements are gathered from an image of the check which is scanned in. Data elements provided directly from the taxpayer include:
- Check Data
    - Check Number

    - Account Number
    - Routing Number
    - Dollar Amount
- Name
- Taxpayer Identification Number (TIN)
- Received Date

Additional information may be included on the check by the taxpayer, but is not specifically requested or required by the system. Typical data elements that may be added to the check are:

- SSN
- Address

Employee – Data elements provided by the employee include:

- RS-PCC user ID and/or
- SEID

Data which will be collected on employees in audit trails:

- SEID
- Date and time of the event
- Type of event
- Subject of the event
- Outcome status

3.a. How will the data collected from sources other than IRS records and the taxpayers be verified for accuracy?

ELVIS returns the ticket number upon the completion of the transaction. This is used to verify that the amount of money that the check was written for is the amount of money deposited. ELVIS returns a deposit ticket summary, which includes the Item Reference Number (generated at the client) and the amount of the transaction that was deposited the previous day. If the amount doesn't reconcile, it is fixed manually. RSPCC goes forward with the ELVIS amount and an Accounting Technician has to submit a debit voucher.

3.b. How will data be checked for completeness?

The transaction data from the remittance will be verified before it is sent to the server. Some of the data will be populated into the system automatically including: amount, check number, account number and routing number. Additionally, users/persons entering the transaction, for example frontline operators or managers, will manually use IDRS or AIS to verify other data elements in the system. It will not let the transaction move forward if data is not entered for each required field. The system will require the user to enter a value for each required field.

3.c. Is the data current? How do you know?

The data in the system is considered current because it is provided directly from the taxpayer and is dated.

4. Are the data elements described in detail and documented? If yes, what is the name of the document?

The data elements are described in the requirements documentation including: the Business System Requirements Report (BSRR), the Design Specification Report, Parts 1 and 2, and the Interface Control Document.

Access to the Data

1. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?

- **Users:** Operators have the ability to create new transactions, edit or delete transactions that have not been submitted, print and view reports.

- **Work Flow Manager:** View the status of the workflows in the system, including workflow to ELVIS, EFTPS and RTR.

- **Managers:** Managers will have access to the SEID numbers of employees who fall under their operational control. View the status of transactions while the data remains in the system.

- **System Administrators:** SA is able to administer user accounts (5081's), apply patches/updates to the platform/ environment under the transmittal process and also work to resolve ITAMS tickets at the request of the business. While the SA has no direct access to the data, the SA has access to archived transmission files that are used in the event that a transmission to one of the application interfaces fails and requires re-transmission. In this scenario the SA may have potential access to taxpayer information. However, all actions by the SA are recorded in the audit logs; the SA does not have access to these logs. They are sent directly to SAAS. The SA is also required to certify that he/she has performed UNAX training annually.

- **Database Administrator:** DBAs control the SYS and SYSTEM accounts in all Oracle databases and therefore require the ability to access all data in the database. These privileges, which include the ability to rewrite, edit and delete if necessary, are required in order for the DBA to fulfill their managerial roles within the system. There are standard auditing functionalities to record the DBA's session.

- **Developers:** Developers will be able to view the status of workflows; however, they would not be able to view transactional data.

- **Public:** RS-PCC does not allow access to the public.

- **Others:** Authorized representatives of TIGTA and C-CIRC will be allowed to review audit logs when necessary to fulfill their auditing responsibilities.

2. How is access to the data by a user determined?

All users requesting access to an IRS system must do so through the OL5081 process. Users are required to complete and OL5081, Information System User Registration/Change Request form, which lists mandatory rules for users of IRS information and information systems. When a user has been approved for access to the application by his/her manager, the OL5081 system sends an email to the user, providing and approval notification. Once approval has been granted, access is restricted to certain individuals based upon their permissions and via the ID and authentication process.

2. a. Are criteria, procedures, controls, and responsibilities regarding access documented?
This control was determined to meet the properties of an organizational common control as defined by Section 2.2.3 Common Controls of this SSP. Access control policy and procedures are formally documented within IRM 10.8.1. As stated within the access control section of the IRM, “Access to information or system resources must be limited to only authorized users, programs, processes, or other systems.” IRM 10.8.1 provides the roles and responsibilities as it pertains to access controls. As stated in the IRM, “This manual provides policies and guidance to be used by IRS organizations to carry out their respective responsibilities in information systems security. It provides guidance on all aspects of security for the protection of information technology resources. It defines responsibilities for the implementation and oversight of the guidance contained herein.” The Business System Requirements Report identifies the roles and Design Specification Report 1 describes how those roles will be implemented.

3. Will users have access to all data on the system or will the user's access be restricted? Explain.
Controls to restrict user access are implemented. Users will need to go through ID and authentication to be able to have access to the system and the data therein. User access to information within the system will be restricted based upon the user’s roles and permissions.

The system is using role-based access control. The role determines the access to the data.

4. What controls are in place to prevent the misuse (e.g. browsing) of data by those having access?
Controls to restrict user access are implemented. Users will first have to request access to the system via the OL5081 process. They will need to go through ID and authentication to be able to have access to the system and the data therein. User access to information within the system will be restricted based upon the users’ roles and minimum necessary permissions. Users will have access to the data that they have input only until the data is batched and transmitted to the server. Data will not be maintained at the workstation. All access will be audited and security logs sent to SAAS. Negative TIN check will be used to prevent browsing of the data. Users will be required to perform annual Unax certification. Since the system resides on a Tier II platform, it will be under the cyber security requirements of Tier II. Physical data (i.e. checks) will be kept in a secured environment (locked cabinet) within the RS-PCC work area. They will be destroyed by shredding within 14 days in this same area.

The system uses minimum necessary permission and role-based access control. The role determines the minimally necessary access to the data.

5.a Do other systems share data or have access to data in this system? If yes, explain.
Yes. RS-PCC relies on several general support systems (GSS) for functionality, but does not share any data elements. RS-PCC currently has the following GSS support:

- MITS-1. IRS Perimeter Security and Network Backbone
- MITS-3. Martinsburg Computing Center (ECC MTB) Domain
- MITS-4. Tennessee Computing Center (ECC MEM)/Memphis Campus Domain.
- MITS-12. Philadelphia Campus Domain
- MITS-17. Workstations/Servers controls and support
- MITS-26. EnterpriseVPN

In addition to the GSSs, RS-PCC shares information electronically with the following three IRS systems:

- **Remittance Transaction Research (RTR)** – This system is an archive tool that provides historical tax payment information. RTR is also used by the IRS to perform payment research. RTR will store remittance transaction data and images for payments processed through RS-PCC. RTR only receives data from RS-PCC and does not provide data.

- **Financial Management Service Electronic Verification and Imaging System (FMS ELVIS)** – The Central Image Research Archive (CIRA) located within the Electronic Verification and Imaging System (ELVIS) is used by the FMS to deposit a remittance in the Federal Reserve Bank (FRB). The FRB has the responsibility to debit the taxpayer account. The RS-PCC system will send remittance transaction data and images to ELVIS after a payment has been processed. RS-PCC will not transmit taxpayer account information to FMS ELVIS. However, the image of the check may also include the Taxpayer Identification Number (TIN) if the information is printed on the check or the Taxpayer has entered the information on the check. ELVIS provides confirmation of the deposit. ELVIS will not have direct access to any of the data in the system.

- **Electronic Federal Tax Payment System (EFTPS)** – EFTPS accepts taxpayer data and remittance information, and transmits that information to the Master File. EFTPS also interfaces with IRACS for accounting and reconciliation purposes. For RS-PCC transactions, EFTPS assigns the document locator number (DLN) and the Trace ID. EFTPS will also interface with IDRS to update the TIF image created by RS-PCC and to journaling information to Interim Revenue Accounting Control System (IRACS). However, they do not have direct access to any of the data in RS-PCC.

5.b. Who will be responsible for protecting the privacy rights of the taxpayers and employees affected by the interface?
As the business owner of the RS-PCC system, Director, Submission Processing, will have ultimate responsibility for protecting the privacy rights of the taxpayers and employees affected by the interfaces.

6.a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, & Other)?
Yes. RS-PCC will send remittance transaction data and images to the Federal Reserve Bank (FRB) via ELVIS. The FRB uses the information to electronically debit the check-writer's account via the Automated Clearing House (ACH) and credits the IRS account in CA$H-LINK. RS-PCC receives data from the Federal Reserve Bank via ELVIS. The FRB returns a confirmed deposit ticket (SF 215) and Item Reference Number (IRN) for each transaction to the RS-PCC system. Data elements provided by the ELVIS include:

- Deposit ticket number (number generated by ELVIS to identify deposits)
- Deposit amount
- Item Reference Number

Authorized representatives of TIGTA and GAO will be allowed to review audit logs when necessary to fulfill their auditing responsibilities.

6.b. How will the data be used by the agency?
The FMS ELVIS/FRB has the responsibility to debit the taxpayer account. The information provided is necessary for this transaction to take place.

As needed or requested, TIGTA and/or GAO may request audit log data to assist with reviews used to ensure that the system is being used and accessed in accordance with standard procedures and to assist with incident response reporting.

6.c. Who is responsible for assuring proper use of the data?
Once audit logs have been reviewed, TIGTA and CSIRC are responsible for ensuring that data is used properly. ELVIS under FMS has the same/equal privacy responsibilities. There is an Interconnection Security Agreement (ISA) between the IRS and FMS that is dated November 6, 2006. IT Security Engineering has determined that RS-PCC will be covered under this ISA.

RS-PCC has two Interface Control Documents (ICD) (each dated April 1, 2007) that establish the general standards, protocols and messages for exchanging information between RS-PCC and RTR and RS-PCC and EFTPS.

Quality reviews of employee work, both random and 100%, are determined by management. Managers, representing the Business Owner, are notified by CSIRC to help determine if the access to the employee work and/or audit trails was legitimate. If the access is determined to be inappropriate, Business Owners are responsible for initiating disciplinary actions. Managers are also responsible for granting and terminating access to data systems and for reviewing the data and audit logs when CSIRC notifies them of a potential inappropriate access.

6.d. How will the system ensure that agencies only get the information they are entitled to under IRC 6103?
FMS ELVIS will only receive data which is necessary to process the transaction. No data elements beyond that which is needed to complete the transaction will be shared. There is an Interconnection Security Agreement (ISA) between the IRS and FMS that is dated November 6, 2006.

Attributes of the Data

1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?
Yes, all data elements are required to accurately apply or correct all payments that are posted to a taxpayer's account.

2.a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

- **Taxpayer:** No, the system will not derive new data for create previously unavailable data about an individual through aggregation.
- **Employee:** No, the system will not derive new data or create previously unavailable data about an individual through aggregation.

2.b. Will the new data be placed in the individual's record (taxpayer or employee)?

- **Taxpayer:** N/A. The information is not new data.

- **Employee:** No new data will be included in the employee's record.

2.c. Can the system make determinations about taxpayers or employees that would not be possible without the new data?

- Taxpayer: No, the system does not have the capability to make independent determinations about taxpayers.
- Employee: No, the system will not be able to make determinations about employees.

2.d. How will the data be verified for relevance and accuracy?
The transaction data from the remittance will be verified before data is sent to the server. Some of the data will be populated into the system automatically using a Magnetic Ink Character Recognition (MICR) machine including: amount, check number, account number and routing number. Additionally, users/persons entering the transaction, for example frontline operators or managers, will manually use IDRS or AIS to verify other data elements in the system.

3.a If the data is being consolidated, what controls are in place to protect the data and prevent unauthorized access? Explain.
Data in the system is not being consolidated.

3.b If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.
N/A. Data in the system is not being consolidated.

4. How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain.
Data is queriable by any data element that is collected in the system, including TIN, Name control, etc..

5. What are the potential effects on the due process rights of taxpayers and employees of:
N/A. The system is not capable of making any determinations on either taxpayers or employees

a. **Consolidation and linkage of files and systems;**

- **Taxpayer:** N/A. The system is not capable of making any determinations on either taxpayers or employees
- **Employee:** N/A. The system is not capable of making any determinations on either taxpayers or employees

b. **Derivation of data;**

- **Taxpayer:** N/A. The system is not capable of making any determinations on either taxpayers or employees
- **Employee:** N/A. The system is not capable of making any determinations on either taxpayers or employees

c. Accelerated information processing and decision making;

- **Taxpayer:** N/A. The system is not capable of making any determinations on either taxpayers or employees
- **Employee:** N/A. The system is not capable of making any determinations on either taxpayers or employees

d. Use of new technologies; N/A. The system is not capable of making any determinations on either taxpayers or employees

How are the effects to be mitigated? N/A.

Maintenance of Administrative Controls

1.a. Explain how the system and its use will ensure equitable treatment of taxpayers and employees.
The system is not able to treat employees or taxpayers differently.

1.b. If the system is operated in more than one site, how will consistent use of the system be maintained at all sites?
RS-PCC has uniform access controls and user policies for all individuals accessing the system from any location.

1.c. Explain any possibility of disparate treatment of individuals or groups.
NA. The system in unable to treat individuals or groups differently, except in regards to levels of access (a function which is determined through the OL5081 process).

2.a. What are the retention periods of data in this system?
Data successfully or unsuccessfully transmitted will be automatically purged via SQL scripts from the server and workstation at different intervals. The physical checks must be destroyed within 14 business days after they are received for processing. The data in the system will be destroyed 14 business days after transmission to RTR.

2.b. What are the procedures for eliminating the data at the end of the retention period?
Where are the procedures documented?
Every transaction submitted to the server from the workstations will have a timestamp on the record in the database. Data successfully or unsuccessfully transmitted will be automatically purged via SQL scripts from the server and workstation at different intervals. The physical checks must be shredded within 14 business days after they are scanned for processing. The shredder must be located within the unit where the scanned checks are securely stored in locked file cabinets. The data in the system will be destroyed after being transmitted to archives, which is after 14 days after they are transferred to RTR. Exhibit 1.15.35-1 in IRM 1.15.35, Records Control Schedule for Tax Administration of Electronic Systems, provides authorization to “destroy these checks and electronic records when they are 1 year old or no longer needed, whichever is sooner.”

The following instructions are being included in all IRMS (i.e., IRM 3.17.278, IRM 21.1.7.5.6.2) and SOPS (Currently, only the SOP for Insolvency Operations) that contain RS-PCC procedures: “The physical checks must be shredded within 14 days after they are scanned for processing. The shredder must be located within the unit where the scanned checks are securely stored in locked file cabinets.” These procedures will be added to other IRMs and SOPs as RS-PCC capabilities are utilized by other Business Operations.

2.c. While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?
N/A. The system does not have the capability to make determinations. Data provided by the taxpayer is considered accurate and timely since it is provided directly from the source. The audit logs are considered to be sufficiently accurate, relevant and timely since they represent a snapshot of activity at a particular given time.

3.a Is the system using technologies in ways that the IRS has not previously employed (e.g. Caller-ID)?
No. RS-PCC does not use any technologies which are new to the IRS technology environment.

3.b How does the use of this technology affect taxpayer/employee privacy?
The technology is not being used in a new way or gathering new types of information, therefore it will have no affect on taxpayer or employee privacy.

4.a Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.
RS-PCC may potentially provide the capability to identify the individual through the TIN and other information which may be present on the paper check. Additionally, if the check contains address information, it may be potentially possible to locate the individual; however, once a check is deleted this is no longer possible. There is not sufficient information gathered on the taxpayer to monitor the individual.

Users are only identified in audit logs by their SEID or IP address, which would need to be matched with other information (not available in the system) in order to identify, locate or monitor the individual.

4.b. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.
No. The system will not have the capability to identify, locate, and monitor groups.

4.c. What controls will be used to prevent unauthorized monitoring?
Controls are in place to restrict access through ID and authentication and restrict permissions through the OL5081 process, which will prevent unauthorized personnel from accessing the system. However, monitoring is not a typical activity of the systems.

5.a Under which Systems of Record Notice (SORN) does the system operate? Provide number and name.
- Treasury/IRS 24.030 CADE/Individual Master File
- Treasury/IRS 24.046 CADE/Business Master File
- Treasury/IRS 34.037 IRS Audit Trail and Security Records System

5.b. If the system is being modified, will the SORN require amendment or revision? Explain.

View other PIAs on IRS.gov